

IN THE UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF: )  
GOOGLE, INC. )  
1600 AMPHITHEATRE PARKWAY )  
MOUNTAIN VIEW, CALIFORNIA 94043)

Magistrate No. 13.0884M

[UNDER SEAL]

AFFIDAVIT

I, Martin Ryan, being duly sworn, do hereby depose and state the following:

**I. INTRODUCTION**

1. I am a Special Agent with the Department of Homeland Security, Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), assigned to assist the Special Agent in Charge, Pittsburgh, Pennsylvania, and have been so employed since July 2004. Prior to my appointment with HSI, I was employed as a United States Border Patrol Agent for approximately five years. As part of my duties as an HSI agent, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of Title 18, United States Code, Sections 2252(a). I have received training in the area of child pornography and child exploitation investigations, and have had the opportunity to observe and review numerous examples of images depicting minors engaged in sexually explicit conduct (as defined in Title 18, United States Code, Section 2256) (hereinafter "child pornography") in a variety of media including computer media. I have also participated in the execution of numerous search warrants which involved child exploitation and/or child pornography offenses.

## **II. PURPOSE OF THE AFFIDAVIT**

2. This affidavit is made in support of a search warrant for records relating to an e-mail account maintained by Google, Inc., headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043. As discussed below, the e-mail account which is the subject of this search warrant, busman0504@gmail.com was identified through the investigation of Mickell Eugene CLOSE, (aka: mrhyde\_31@yahoo.com). As set forth herein, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 2252(a), regarding the possession, transportation and receipt of visual depictions involving the use of a minor engaging in sexually explicit conduct, are located within information associated with this e-mail account.

3. Because the purpose of this affidavit is to set forth only the facts necessary to establish probable cause for a search warrant for the pertinent email account, I have not described all the facts and circumstances of which I am aware. Facts not set forth herein are not relied upon in support of my conclusion that probable cause exists. Where statements of others are set forth in this affidavit, they are set forth in substance and in part.

## **III. STATUTORY AUTHORITY**

4. The legal authority for this search warrant application is derived from Title 18, United States Code, chapter 121, §§ 2701-11, entitled, "stored wire and electronic communications and transactional records access."

5. 18 U.S.C. § 2703(c)(A) allows for nationwide service of process of search warrants for the contents of electronic communications. Pursuant to 18 U.S.C. § 2703, as

amended by the USA PATRIOT Act, Section 220, a government entity may require a provider of an electronic communication service or a remote computing service to disclose a record or other information pertaining to a subscriber or customer of such service pursuant to a warrant issued using procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation.

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i). This Court has jurisdiction over the offense under investigation because the email account busman0504@gmail.com has been accessed from Internet Protocol (“IP”) addresses in the Western District of Pennsylvania.

7. 18 U.S.C. § 2703 further states in part:

(a) Contents of Wire or Electronic Communications in Electronic Storage.

– A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communication system for more

than one hundred and eighty days by the means available under subsection (b) of this section.

(b) Contents of Wire or Electronic Communications in a Remote Computing Service. – (1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2)<sup>1</sup> of this subsection –

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant....

8. 18 U.S.C. 2703(c)(2) adds that a provider of an electronic communication service or remote computer service must also provide, without notice to the customer, the name, address, connection records, length of service, and means of payment pursuant to a search warrant.

9. 18 U.S.C. § 2252(a) prohibits a person from knowingly transporting, shipping, receiving, distributing, possessing, or accessing with intent to view, any visual depiction using any means or facility of interstate or foreign commerce or that has been

---

<sup>1</sup> Paragraph (2) of 18 U.S.C. § 2703 states, "[p]aragraph 1 is applicable with respect to any wire or electronic communication that is held or maintained on that service-

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing."

mailed, or has been shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means, including by computer, if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct. 18 U.S.C. § 2256(2)(A) provides that sexually explicit conduct means actual or simulated sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, bestiality, masturbation, sadistic or masochistic abuse; or the lascivious exhibition of the genitals or pubic area of any person.

#### **IV. FACTS ESTABLISHING PROBABLE CAUSE**

10. In June 2012, the HSI Columbus, Ohio office received information from the HSI Philadelphia, Pennsylvania office regarding an individual, known only by profile names "mrhyde\_31" ([mr\\_hyde31@yahoo.com](mailto:mr_hyde31@yahoo.com)) and loverboy31 ([loverboy\\_31@rocketmail.com](mailto:loverboy_31@rocketmail.com)). This individual was uploading images suspected of containing child pornography to the file-sharing website [www.ingsrc.ru](http://www.ingsrc.ru). Both profile pages contained folders (two of which were password protected) which were titled: "my step daughter xxx", "my hot niece xxx", "my stepdaughter", "my little stepdaughter", "my hot niece", "Stepdaughter 2", "Stepdaughter 1", and "niece." These folders contained at least 100 photos, mainly of three minor females in various stages of undress, fully clothed or clothed photos focused on their buttocks or genitalia.

11. On September 20, 2012, the contents of e-mail account [mrhyde\\_31@yahoo.com](mailto:mrhyde_31@yahoo.com) were received from Yahoo pursuant to a federal search warrant. A review of the e-mails and attachments showed that [mrhyde\\_31@yahoo.com](mailto:mrhyde_31@yahoo.com) sent and received e-mails containing images and/or videos depicting minors engaged in sexually

explicit conduct or posed in a sexually explicit manner. After further investigation, HSI Columbus agents subsequently arrested Mickell Eugene CLOSE, for violations of Title 18, United States Code Sections 2251(a) and 2252; production of child pornography and receipt, possession and/or distribution of child pornography. CLOSE pleaded guilty to one count of production of child pornography, in violation of Title 18, United States Code, Section 2251, and was sentenced on July 18, 2013, to 25 years incarceration.

12. Three federal search warrants were conducted on the contents of three (3) email accounts used by CLOSE: mrhyde\_31@yahoo.com, loverboy\_31@rocketmail.com, and hyde\_mike@rocketmail.com. CLOSE used each of the three accounts to send and/or receive images and videos depicting child pornography to other e-mail accounts throughout the world. Agents reviewed the target e-mail addresses. HSI Summonses were sent to the various target e-mail providers to identify login IP addresses used by each e-mail address involved in the exchanges with CLOSE. After receiving the list of log-in IP addresses, HSI Summonses were sent to the Internet Service Providers (ISP) in an attempt to identify the physical location of the violators. The most recent IP address used to access the e-mail account was summonsed.

13. HSI agents in Columbus reviewed "To:" and "Sent:" records for the three above-referenced email accounts associated with Mickell Eugene CLOSE. Upon examination of those accounts, the HSI agents were able to determine that, between June and September of 2012, the email address kennyv101975@yahoo.com had been involved in the email exchanges and had received three emails which the agents believe contained child pornography. I have reviewed those emails which were sent to kennyv101975@yahoo.com, which included the following:

(a) An email string that was sent as a Reply to email address fashion-model-art@hotmail.com from mrhyde\_31@yahoo.com, with the subject "Re: little girls". The email communication was part of a larger email string which was sent to several email addresses, including kennyv101975@yahoo.com. The original email of the string was sent on June 28, 2012 21:32:53 (-0500) from ronlikesit@gmail.com to several email addresses, including kennyv101975@yahoo.com. The email contained a video attachment, labeled "!!!NEW!!! Daddy's Girl - 12yo Girl Give's Alittle Head". The body of the email reads: "How many of you have little girls or know of some little girls you love to look at Reply". The video "!!!NEW!!! Daddy's Girl - 12yo Girl Give's Alittle Head", is two minutes and 34 seconds in length. The writing on the video screen reads, "little sweetie gives head", and depicts a mostly naked adult male laying on his back on a bed, wearing only women's panties. A naked female, approximately 12-13 years of age is laying in between the male's legs. The male encourages the girl to perform oral sex on him, saying, "Seriously, it's not embarrassing sweetie. Do what I just showed you on him. I just blew your brother - that's different." The girl says, "Your legs...they scratch me". The man replies, "Sorry, I'm a man. I have coarser hair". It appears as though another person is holding the camera in order to record the event. The female performs oral sex on the male. A few seconds before the video ends, the male says, "OK, it's time to fuck".

(b) An email communication from email address mj.halal92@gmail.com to several email addresses, including kennyv101975@yahoo.com, with the subject "Trades". The email was sent September 5, 2012, 4:54 PM. The message in the body of the email reads, "Wanna trade? :) i got more, videos aswell.". Attached to the email are six photographs

depicting a young female, approximately 3 years of age, laying naked except for a shirt. The girl's legs are apart, exposing her genital area. An adult female has her hand on the inside of the young girl's leg.

14. On August 1, 2013, HSI Columbus summonsed registration information and IP log on data from Yahoo Inc., for email address kennyv101975@yahoo.com. On August 19, 2013, HSI Columbus received a response to that summons, with Yahoo Inc., indicating in the response that IP Address 74.111.182.88 was used to access email address kennyv101975@yahoo.com on August 12, 2013 at 19:30:24 (GMT). Yahoo Inc. records indicate that the email account for kennyv101975@yahoo.com also reported an alternate email address of studman101975@yahoo.com. That IP address is assigned to a Verizon customer.

15. On September 26, 2013, HSI Columbus sent a Customs Summons to Verizon for the most recent log-on IP address used by the subject, for IP Address 74.111.182.88, most recently used on August 12, 2013, at 19:30:24 (GMT). On that same date, information received from Verizon showed that the IP address is registered to Mark CHASEY at 504 Crescent Boulevard Extension, Crescent, Pennsylvania 10546.

16. SA Connelly performed a Google internet database query for email address kennyv101975@yahoo.com. The Google search returned a record of a profile on the image file sharing website www.imgsrc.ru, with the User Name: "HAPPYSTEPDADDY37". As stated above, this is the same file sharing website that was being accessed by CLOSE when CLOSE was uploading child pornography images. The account for kennyv101975@yahoo.com was registered with imgsrc.ru on May 7, 2012. There was a caption attached to the profile, reading, "User info: I am a very happy



and lucky step daddy”. No additional pages, photographs, videos, or comments appear to be associated with the profile.

17. On October 7, 2013, the Crescent Township, PA Police Department and HSI Pittsburgh executed a federal search warrant at 504 Crescent Boulevard Extension, Crescent, Pennsylvania 15046, the residence of Mark A. CHASEY. CHASEY was encountered in the residence and agreed to speak with agents without the presence of an attorney.

18. SA’s Robert Connelly and Martin Ryan interviewed CHASEY at the residence. CHASEY admitted to receiving, viewing and sending email communications containing child pornography, to email addresses for unknown persons he “met” on the image posting website [www.imgsrc.ru](http://www.imgsrc.ru). CHASEY admitted to having a profile on [www.imgsrc.ru](http://www.imgsrc.ru) under the profile name HAPPYSTEPDADDY37.

19. CHASEY admitted to having email address [kennyv101975@yahoo.com](mailto:kennyv101975@yahoo.com), using fictitious name “Kenny VAROS”. CHASEY admitted to having email contact and trading photographs and videos depicting child pornography with email address [mrhyde\\_31@yahoo.com](mailto:mrhyde_31@yahoo.com). CHASEY said that he is sexually interested in girls between the ages of 12-16 years of age. CHASEY said that when viewing images and videos of non-child pornography and child pornography he received from others, he would view and delete the material from his internet web browser history, but not necessarily from Yahoo email account [kennyv109175@yahoo.com](mailto:kennyv109175@yahoo.com). CHASEY described that he would delete the internet browser’s cache, saying, “Tools, History, Delete”, to describe the actions taken to accomplish the deleting of child pornography material.

20. CHASEY claimed that he has received "a couple hundred" emails containing child pornography "over the years". CHASEY claimed that in email address kennyv101975@yahoo.com, "under 100" emails containing child pornography could be found.

21. CHASEY granted consent for HSI special agents to access and assume control of email address kennyv10975@yahoo.com, and gave agents the password for the email account. SA Connelly accessed and performed a brief review of email messages and attachments, some of which contained child pornography. SA Connelly observed that a second email address was listed as an alternate communication, studman101975@yahoo.com. CHASEY admitted that this email address was also his, and that he had previously used that email address to receive, view and send images and videos depicting child pornography to other email addresses for unknown persons. CHASEY claimed that he had deleted the email account for studman101975@yahoo.com approximately two years prior.

22. CHASEY granted consent for HSI special agents to access and assume control of email address studman101975@yahoo.com, and gave agents the password for the email account, which had not been deleted as CHASEY had asserted. SA Connelly accessed and performed a brief review of email messages and attachments, some of which contained child pornography. CHASEY said that he originally used email address studman101975@yahoo.com to receive, view and send child pornography, but that he continuously received pornographic images and videos that CHASEY found very offensive (ie: bestiality), from an email address for an unknown person. CHASEY claimed that he emailed the person to stop sending material that CHASEY found

offensive, but CHASEY continued to receive the emails. In an effort to not receive further emails from this unknown person, CHASEY said he created email address kennyv101975@yahoo.com. CHASEY said that he did not attempt to report to law enforcement or any other entity, the receipt of any email communications containing child pornography or other material he deemed offensive.

23. On October 9, 2013, at the HSI Pittsburgh office, SA Connelly performed a review of email address studman101975@yahoo.com, and discovered email communications containing child pornography between CHASEY and other email addresses for unknown persons. One such email was sent from CHASEY using studman101975@yahoo.com to CHASEY using kennyv101975@yahoo.com. The email contained 14 images of a pubescent juvenile female, approximately age 13-14, laying nude on a bed. Several of the images are of the female spreading her legs in order to expose her vagina. A few of the images depict the female inserting objects into her vagina.

24. On October 11, 2013, SA Connelly continued a review of email account studman101975@yahoo.com. An alternate email address listed on the account is busman0504@yahoo.com (CHASEY holds a bus operator endorsement on his Pennsylvania Driver's license and is the Director of Transportation for bussing students at the Hopewell, PA School District, and "0504" is associated with is month and day of birth: May 4, 1965).

25. During his initial interview on October 7, 2013, CHASEY gave SA's Connelly and Ryan points of contact to be reached, including phone numbers and email addresses. Two such email addresses were m.chasey0504@verizon.net and

garbageaccount0504@verizon.net.

26. SA Connelly performed a search within email account studman101975@yahoo.com for email communications using the term "busman0504". The email search returned several email communications to and from email address busman0504@gmail.com. One such email communication was originally sent from email jdud09@gmail.com (aka: Jason Duldý) on 10/07/2009 at 8:28 a.m. to busman0504@gmail.com. The email contained an attached video labeled, "In Alex's ass". The video is 50 seconds in length, and depicts a prepubescent female laying on her back, being anally penetrated by an adult male. The prepubescent female is then shown kneeling and bent over, again being anally penetrated. On 11/09/2009 at 7:17 a.m., email address busman0504@gmail.com forwarded this email to studman101975@yahoo.com.

27. On August 27, 2013, HSI Columbus, OH sent a Preservation Request letter to Yahoo, Inc., pursuant to Electronic Communications Privacy Act (ECPA) 18 USC 2703, for the preservation of records relating to email address kennyv101975@yahoo.com, for a period of 90 days.

28. On October 9, 2013, SA Ryan sent a Preservation Request letter to Yahoo, Inc., pursuant to Electronic Communications Privacy Act (ECPA) 18 USC 2703, for the preservation of records relating to email addresses kennyv101975@yahoo.com and studman101975@yahoo.com, for a period of 90 days.

29. On October 11, 2013, SA Ryan sent a Preservation Request letter to Yahoo, Inc., and Google (Gmail) pursuant to Electronic Communications Privacy Act (ECPA) 18 USC 2703, for the preservation of records relating to email addresses busman0504@gmail.com and busman0504@yahoo.com, for a period of 90 days.

**V. INFORMATION THAT MAY BE AVAILABLE FROM GOOGLE, INC.**

30. In my training and experience, I have learned that Google, Inc. provides a variety of on-line services, including electronic mail (“e-mail”) access, to the general public. Google, Inc. allows subscribers to obtain e-mail accounts at the domain name gmail.com like the e-mail account listed in Attachment A. Subscribers obtain an account by registering with Google, Inc.. During the registration process, Google, Inc. asks subscribers to provide basic personal information. Therefore, the computers of Google, Inc. are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for Google, Inc. subscribers) and information concerning subscribers and their use of Google, Inc. services, such as account access information, e-mail transaction information, and account application information.

31. In general, an e-mail that is sent to a Google, Inc. subscriber is stored in the subscriber’s “mail box” on Google, Inc. servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Google, Inc. servers indefinitely.

32. When the subscriber sends an e-mail, it is initiated at the user’s computer, transferred via the Internet to Google, Inc.’s servers, and then transmitted to its end destination. Google, Inc. often saves a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from the Google, Inc. server, the e-mail can remain on the system indefinitely.

33. A sent or received e-mail typically includes the content of the message, source and destination addresses, the date and time at which the e-mail was sent, and the size and length of the e-mail. If an e-mail user writes a draft message but does not send

it, that message may also be saved by Google, Inc. but may not include all of these categories of data.

34. A Google, Inc. subscriber can also store files, including e-mails, address books, contact or buddy lists, calendar data, pictures, and other files, on servers maintained and/or owned by Google, Inc.

35. Subscribers to Google, Inc. might not store on their home computers copies of the e-mails stored in their Google, Inc. account. This is particularly true when they access their Google, Inc. account through the web, or if they do not wish to maintain particular e-mails or files in their residence.

36. In general, e-mail providers like Google, Inc. ask each of their subscribers to provide certain personal identifying information when registering for an e-mail account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

37. E-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google, Inc.'s website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to

the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

38. In some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

#### **VI. INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

39. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment A. Upon receipt of the information described in Section I of Attachment A, government-authorized persons will review that information to locate the items described in Section II of Attachment A.

#### **VII. CONCLUSION**

40. Based on the aforementioned factual information, and my training and experience, your affiant respectfully submits that there is probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a) are located on the computer systems in the control of Google, Inc.

41. It is further respectfully requested that this Court issue an Order sealing, until further order of Court, all papers submitted in support of this Application, including

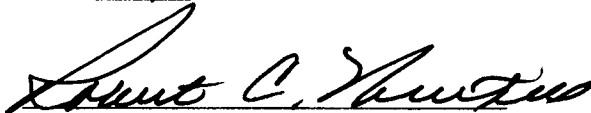
the Application, Affidavit and attachments thereto, and the Search Warrant, and the requisite inventory notice (with the exception of one copy of the warrant and inventory notice that will be left at Google, Inc., 1600 Amphitheatre Parkway, Mountain View, California 94043). Sealing is necessary because the items and information to be seized are relevant to an ongoing investigation and premature disclosure of the contents of this Affidavit and related documents may have a negative impact on this continuing investigation and may jeopardize its effectiveness.

42. The above information is true and correct to the best of my knowledge, information and belief.



MARTIN RYAN  
Special Agent  
Department of Homeland Security  
ICE-Homeland Security Investigations

SUBSCRIBED TO AND SWORN BEFORE ME  
THIS 17 DAY OF October, 2013



ROBERT C. MITCHELL  
United States Magistrate Judge



## **ATTACHMENT A**

### **Particular Things to be Seized**

#### **Section I - Information to be disclosed by Google, Inc.:**

To the extent that the information described is within the possession, custody, or control of Google, Inc., Google, Inc. is required to disclose the following information to the government for the email account busman0504@gmail.com:

- a. The contents of all e-mails and instant messages stored in the account, including copies of e-mails and instant messages sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail or instant message, the date and time at which each e-mail or instant message was sent, and the size and length of each e-mail or instant message;
- b. All records or other information regarding the identification of the e-mail or instant messaging account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

d. All records pertaining to communications between Google, Inc., and any person regarding the account, including contacts with support services and records of actions taken.

**Section II - Information to be seized by the government:**

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. Section 2252(a), including, for each account or identifier listed on Section I, information pertaining to the following matters:

- a. The possession, transportation, or receipt of visual depictions involving the use of a minor engaging in sexually explicit conduct;
- b. Records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts.